The Plünnecke-Ruzsa Inequality

Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson

March 17, 2025

Abstract

We formalise Plünnecke's inequality and the Plünnecke-Ruzsa inequality, following the notes by Timothy Gowers: "Introduction to Additive Combinatorics" (2022) for the University of Cambridge. To this end, we first introduce basic definitions and prove elementary facts on sumsets and difference sets. Then, we show two versions of the Ruzsa triangle inequality. We follow with a proof due to Petridis [1].

Contents

Acknowledgements The authors were supported by the ERC Advanced Grant ALEXANDRIA (Project 742178) funded by the European Research Council.

1 The Plünnecke-Ruzsa Inequality

Authors: Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson, University of Cambridge.

We formalise Plünnecke's inequality and the Plünnecke-Ruzsa inequality, following the notes by Timothy Gowers: "Introduction to Additive Combinatorics" (2022) for the University of Cambridge. To this end, we first introduce basic definitions and prove elementary facts on sumsets and difference sets. Then, we show (two versions of) the Ruzsa triangle inequality. We follow with a proof due to Petridis.

theory *Pluennecke-Ruzsa-Inequality*
  imports
    Jacobson-Basic-Algebra.Ring-Theory
    Complex-Main

begin

notation *plus* (**infixl** ‹+› *65*)
notation *minus* (**infixl** ‹−› *65*)
unbundle *uminus-syntax*

1.1 Key definitions (sumset, difference set) and basic lemmas

Working in an arbitrary Abelian group, with additive syntax

locale *additive-abelian-group* = *abelian-group* G (⊕) **0**
  for G **and** *addition* (**infixl** ‹⊕› *65*) **and** *zero* (‹**0**›)

begin

abbreviation *G-minus*:: $'a \Rightarrow 'a \Rightarrow 'a$ (**infixl** ‹⊖› *70*)
  where $x \ominus y \equiv x \oplus$ *inverse* y

lemma *inverse-closed*: $x \in G \Longrightarrow$ *inverse* $x \in G$
  ⟨*proof*⟩

1.1.1 Sumsets

inductive-set *sumset* :: $'a$ *set* $\Rightarrow$ $'a$ *set* $\Rightarrow$ $'a$ *set* **for** A B
  where
    sumsetI[*intro*]: $[\![a \in A;\ a \in G;\ b \in B;\ b \in G]\!] \Longrightarrow a \oplus b \in$ *sumset* A B

lemma *sumset-eq*: *sumset* A $B = \{c.\ \exists\, a \in A \cap G.\ \exists\, b \in B \cap G.\ c = a \oplus b\}$
  ⟨*proof*⟩

lemma *sumset*: *sumset* A $B = (\bigcup a \in A \cap G.\ \bigcup b \in B \cap G.\ \{a \oplus b\})$
  ⟨*proof*⟩

lemma *sumset-subset-carrier*: *sumset* A $B \subseteq G$
⟨*proof*⟩

lemma *sumset-Int-carrier* [*simp*]: *sumset* A $B \cap G$ = *sumset* A B
⟨*proof*⟩

lemma *sumset-mono*: $[\![A' \subseteq A; B' \subseteq B]\!] \Longrightarrow$ *sumset* A' $B' \subseteq$ *sumset* A B
⟨*proof*⟩

lemma *sumset-insert1*: *NO-MATCH* $\{\}$ $A \Longrightarrow$ *sumset* (*insert* x A) B = *sumset* $\{x\}$ $B \cup$ *sumset* A B
⟨*proof*⟩

lemma *sumset-insert2*: *NO-MATCH* $\{\}$ $B \Longrightarrow$ *sumset* A (*insert* x B) = *sumset* A $\{x\} \cup$ *sumset* A B
⟨*proof*⟩

lemma *sumset-subset-Un1*: *sumset* $(A \cup A')$ B = *sumset* A $B \cup$ *sumset* A' B
⟨*proof*⟩

lemma *sumset-subset-Un2*: *sumset* A $(B \cup B')$ = *sumset* A $B \cup$ *sumset* A B'
⟨*proof*⟩

lemma *sumset-subset-insert*: *sumset* A $B \subseteq$ *sumset* A (*insert* x B) *sumset* A $B \subseteq$ *sumset* (*insert* x A) B
⟨*proof*⟩

lemma *sumset-subset-Un*: *sumset* A $B \subseteq$ *sumset* A $(B \cup C)$ *sumset* A $B \subseteq$ *sumset* $(A \cup C)$ B
⟨*proof*⟩

lemma *sumset-empty* [*simp*]: *sumset* A $\{\} = \{\}$ *sumset* $\{\}$ $A = \{\}$
⟨*proof*⟩

lemma *sumset-empty'*:
assumes $A \cap G = \{\}$
shows *sumset* B $A = \{\}$ *sumset* A $B = \{\}$
⟨*proof*⟩

lemma *sumset-is-empty-iff* [*simp*]: *sumset* A $B = \{\} \longleftrightarrow A \cap G = \{\} \vee B \cap G = \{\}$
⟨*proof*⟩

lemma *sumset-D* [*simp*]: *sumset* A $\{\mathbf{0}\} = A \cap G$ *sumset* $\{\mathbf{0}\}$ $A = A \cap G$
⟨*proof*⟩

lemma *sumset-Int-carrier-eq* [*simp*]: *sumset* A $(B \cap G)$ = *sumset* A B *sumset* $(A \cap G)$ B = *sumset* A B

⟨*proof*⟩

lemma *sumset-assoc*:
shows $sumset\ (sumset\ A\ B)\ C = sumset\ A\ (sumset\ B\ C)$
⟨*proof*⟩

lemma *sumset-commute*:
shows $sumset\ A\ B = sumset\ B\ A$
⟨*proof*⟩

lemma *finite-sumset*:
assumes $finite\ A$ $finite\ B$ **shows** $finite\ (sumset\ A\ B)$
⟨*proof*⟩

lemma *finite-sumset'*:
assumes $finite\ (A \cap G)$ $finite\ (B \cap G)$
shows $finite\ (sumset\ A\ B)$
⟨*proof*⟩

lemma *sumsetdiff-sing*: $sumset\ (A - B)\ \{x\} = sumset\ A\ \{x\} - sumset\ B\ \{x\}$
⟨*proof*⟩

lemma *card-sumset-singleton-eq*:
assumes $finite\ A$ **shows** $card\ (sumset\ A\ \{a\}) = (if\ a \in G\ then\ card\ (A \cap G)\ else\ 0)$
⟨*proof*⟩

lemma *card-sumset-le*:
assumes $finite\ A$ **shows** $card\ (sumset\ A\ \{a\}) \leq card\ A$
⟨*proof*⟩

lemma *infinite-sumset-aux*:
assumes $infinite\ (A \cap G)$
shows $infinite\ (sumset\ A\ B) \longleftrightarrow B \cap G \neq \{\}$
⟨*proof*⟩

lemma *infinite-sumset-iff*:
shows $infinite\ (sumset\ A\ B) \longleftrightarrow infinite\ (A \cap G) \wedge B \cap G \neq \{\} \vee A \cap G \neq \{\} \wedge infinite\ (B \cap G)$
⟨*proof*⟩

lemma *card-le-sumset*:
assumes A: $finite\ A$ $a \in A$ $a \in G$
and B: $finite\ B$ $B \subseteq G$
shows $card\ B \leq card\ (sumset\ A\ B)$
⟨*proof*⟩

lemma *card-sumset-0-iff'*: $card\ (sumset\ A\ B) = 0 \longleftrightarrow card\ (A \cap G) = 0 \vee card\ (B \cap G) = 0$

⟨*proof*⟩

lemma *card-sumset-0-iff*:
assumes $A \subseteq G$ $B \subseteq G$
shows $card\ (sumset\ A\ B) = 0 \longleftrightarrow card\ A = 0 \lor card\ B = 0$
⟨*proof*⟩

lemma *card-sumset-leq*:
assumes $A \subseteq G$
shows $card(sumset\ A\ A) \leq Suc(card\ A)\ choose\ 2$
⟨*proof*⟩

1.1.2 Iterated sumsets

definition *sumset-iterated* :: $'a\ set \Rightarrow nat \Rightarrow 'a\ set$
where $sumset\text{-}iterated\ A\ r \equiv Finite\text{-}Set.fold\ (sumset \circ (\lambda\text{-}.\ A))\ \{\mathbf{0}\}\ \{..<r\}$

lemma *sumset-iterated-0* [*simp*]: $sumset\text{-}iterated\ A\ 0 = \{\mathbf{0}\}$
⟨*proof*⟩

lemma *sumset-iterated-Suc* [*simp*]: $sumset\text{-}iterated\ A\ (Suc\ k) = sumset\ A\ (sumset\text{-}iterated\ A\ k)$
(**is** *?lhs* = *?rhs*)
⟨*proof*⟩

lemma *sumset-iterated-2*:
shows $sumset\text{-}iterated\ A\ 2 = sumset\ A\ A$
⟨*proof*⟩

lemma *sumset-iterated-r*: $r > 0 \Longrightarrow sumset\text{-}iterated\ A\ r = sumset\ A\ (sumset\text{-}iterated\ A\ (r-1))$
⟨*proof*⟩

lemma *sumset-iterated-subset-carrier*: $sumset\text{-}iterated\ A\ k \subseteq G$
⟨*proof*⟩

lemma *finite-sumset-iterated*: $finite\ A \Longrightarrow finite\ (sumset\text{-}iterated\ A\ r)$
⟨*proof*⟩

lemma *sumset-iterated-empty*: $r>0 \Longrightarrow sumset\text{-}iterated\ \{\}\ r = \{\}$
⟨*proof*⟩

1.1.3 Difference sets

inductive-set *minusset* :: $'a\ set \Rightarrow 'a\ set$ **for** A
where
minussetI[*intro*]: $[\![a \in A;\ a \in G]\!] \Longrightarrow inverse\ a \in minusset\ A$

lemma *minusset-eq*: $minusset\ A = inverse\ \text{`}\ (A \cap G)$
⟨*proof*⟩

abbreviation *differenceset* A $B \equiv$ *sumset* A (*minusset* B)

lemma *minusset-is-empty-iff* [*simp*]: *minusset* $A = \{\} \longleftrightarrow A \cap G = \{\}$
⟨*proof*⟩

lemma *minusset-triv* [*simp*]: *minusset* $\{\mathbf{0}\} = \{\mathbf{0}\}$
⟨*proof*⟩

lemma *minusset-subset-carrier*: *minusset* $A \subseteq G$
⟨*proof*⟩

lemma *minus-minusset* [*simp*]: *minusset* (*minusset* A) $= A \cap G$
⟨*proof*⟩

lemma *card-minusset* [*simp*]: *card* (*minusset* A) $=$ *card* $(A \cap G)$
⟨*proof*⟩

lemma *card-minusset'*: $A \subseteq G \Longrightarrow$ *card* (*minusset* A) $=$ *card* A
⟨*proof*⟩

lemma *diff-minus-set*:
differenceset (*minusset* A) $B =$ *minusset* (*sumset* A B) (**is** *?lhs* $=$ *?rhs*)
⟨*proof*⟩

lemma *differenceset-commute* [*simp*]:
shows *minusset* (*differenceset* B A) $=$ *differenceset* A B
⟨*proof*⟩

lemma *card-differenceset-commute*: *card* (*differenceset* B A) $=$ *card* (*differenceset* A B)
⟨*proof*⟩

lemma *minusset-distrib-sum*:
shows *minusset* (*sumset* A B) $=$ *sumset* (*minusset* A) (*minusset* B)
⟨*proof*⟩

lemma *minusset-iterated-minusset*: *sumset-iterated* (*minusset* A) $k =$ *minusset* (*sumset-iterated* A k)
⟨*proof*⟩

lemma *card-sumset-iterated-minusset*:
card (*sumset-iterated* (*minusset* A) k) $=$ *card* (*sumset-iterated* A k)
⟨*proof*⟩

lemma *finite-minusset*: *finite* $A \Longrightarrow$ *finite* (*minusset* A)
⟨*proof*⟩

lemma *finite-differenceset*: *finite* $A \Longrightarrow$ *finite* $B \Longrightarrow$ *finite* (*differenceset* A B)
⟨*proof*⟩

1.2 The Ruzsa triangle inequality

lemma *Ruzsa-triangle-ineq1*:
assumes U: *finite* U $U \subseteq G$
and V: *finite* V $V \subseteq G$
and W: *finite* W $W \subseteq G$
shows (*card* U) $*$ *card*(*differenceset* V W) $\leq$ *card* (*differenceset* U V) $*$ *card* (*differenceset* U W)
⟨*proof*⟩

definition *Ruzsa-distance*:: $'a$ *set* $\Rightarrow$ $'a$ *set* $\Rightarrow$ *real*
where *Ruzsa-distance* A $B \equiv$ *card*(*differenceset* A B)/(*sqrt*(*card* A) $*$ *sqrt*(*card* B))

lemma *Ruzsa-triangle-ineq2*:
assumes U: *finite* U $U \subseteq G$ $U \neq \{\}$
and V: *finite* V $V \subseteq G$
and W: *finite* W $W \subseteq G$
shows *Ruzsa-distance* V $W \leq$ (*Ruzsa-distance* V U) $*$ (*Ruzsa-distance* U W)
⟨*proof*⟩

1.3 Petridis's proof of the Plünnecke-Ruzsa inequality

lemma *Plu-2-2*:
assumes $K0$: *card* (*sumset* $A0$ B) $\leq K0 *$ *real* (*card* $A0$)
and $A0$: *finite* $A0$ $A0 \subseteq G$ $A0 \neq \{\}$
and B: *finite* B $B \subseteq G$ $B \neq \{\}$
obtains A K
where $A \subseteq A0$ $A \neq \{\}$ $0 < K$ $K \leq K0$
and $\bigwedge C.$ $C \subseteq G \Longrightarrow$ *finite* $C \Longrightarrow$ *card* (*sumset* A (*sumset* B C)) $\leq K *$ *real* (*card*(*sumset* A C))
⟨*proof*⟩

lemma *Cor-Plu-2-3*:
assumes K: *card* (*sumset* A B) $\leq K *$ *real* (*card* A)
and A: *finite* A $A \subseteq G$ $A \neq \{\}$
and B: *finite* B $B \subseteq G$
obtains A' **where** $A' \subseteq A$ $A' \neq \{\}$
$\bigwedge r.$ *card* (*sumset* A' (*sumset-iterated* B r)) $\leq K\hat{}r *$ *real* (*card* A')
⟨*proof*⟩

The following Corollary of the above is an important special case, also referred to as the original version of Plünnecke's inequality first shown by Plünnecke.

lemma *Cor-Plu-2-3-Pluennecke-ineq*:

assumes *K*: *card* (*sumset A B*) ≤ *K* ∗ *real* (*card A*)
and *A*: *finite A A* ⊆ *G A* ≠ {}
and *B*: *finite B B* ⊆ *G*
shows *real* (*card* (*sumset-iterated B r*)) ≤ *K* ^ *r* ∗ *real* (*card A*)
⟨*proof*⟩

Special case where $B = A$

lemma *Cor-Plu-2-3-1*:
assumes *K*: *card* (*sumset A A*) ≤ *K* ∗ *real* (*card A*)
and *A*: *finite A A* ⊆ *G A* ≠ {}
shows *card* (*sumset-iterated A r*) ≤ *K*^*r* ∗ *real* (*card A*)
⟨*proof*⟩

Special case where $B = - A$

lemma *Cor-Plu-2-3-2*:
assumes *K*: *card* (*differenceset A A*) ≤ *K* ∗ *real* (*card A*)
and *A*: *finite A A* ⊆ *G A* ≠ {}
shows *card* (*sumset-iterated A r*) ≤ *K*^*r* ∗ *real* (*card A*)
⟨*proof*⟩

The following result is known as the Plünnecke-Ruzsa inequality (Theorem 2.5 in Gowers's notes). The proof will make use of the Ruzsa triangle inequality.

theorem *Pluennecke-Ruzsa-ineq*:
assumes *K*: *card* (*sumset A B*) ≤ *K* ∗ *real* (*card A*)
and *A*: *finite A A* ⊆ *G A* ≠ {}
and *B*: *finite B B* ⊆ *G*
and *0* < *r 0* < *s*
shows *card* (*differenceset* (*sumset-iterated B r*) (*sumset-iterated B s*)) ≤ *K*^(*r*+*s*) ∗ *real*(*card A*)
⟨*proof*⟩

The following is an alternative version of the Plünnecke-Ruzsa inequality (Theorem 2.1 in Gowers's notes).

theorem *Pluennecke-Ruzsa-ineq-alt*:
assumes *finite A A* ⊆ *G*
and *card* (*sumset A A*) ≤ *K* ∗ *real* (*card A*) *r* > *0 s* > *0*
shows *card* (*differenceset* (*sumset-iterated A r*) (*sumset-iterated A s*)) ≤ *K*^(*r*+*s*) ∗ *real*(*card A*)
⟨*proof*⟩

theorem *Pluennecke-Ruzsa-ineq-alt-2*:
assumes *finite A A* ⊆ *G*
and *card* (*differenceset A A*) ≤ *K* ∗ *real* (*card A*) *r* > *0 s* > *0*
shows *card* (*differenceset* (*sumset-iterated A r*) (*sumset-iterated A s*)) ≤ *K*^(*r*+*s*) ∗ *real*(*card A*)
⟨*proof*⟩

end

1.4 Supplementary material on sumsets for sets of integers: basic inequalities

lemma *moninv-int*: *monoid.invertible UNIV* (+) *0 u* **for** *u*::*int*
⟨*proof*⟩

interpretation *int*: *additive-abelian-group UNIV* (+) *0*::*int*
⟨*proof*⟩

lemma *card-sumset-geq1*:
assumes *A*: $A \neq \{\}$ *finite A* **and** *B*: $B \neq \{\}$ *finite B*
shows *card*(*int.sumset A B*) $\geq$ (*card A*) + (*card B*) − *1*
⟨*proof*⟩

lemma *card-sumset-geq2*:
shows *card*(*int.sumset A A*) $\geq$ *2* ∗ (*card A*) − *1*
⟨*proof*⟩

end

References

[1] G. Petridis. The Plünnecke–Ruzsa inequality: An overview. In M. B. Nathanson, editor, *Combinatorial and Additive Number Theory*, pages 229–241. Springer, 2014.